## REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-26 are pending in the application. The Examiner additionally stated that claims 1-26 are rejected. By this communication, claims 1, 7, 10, 14, 17, 21-22, and 26 are amended. Hence, claims 1-26 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

**Information Disclosure Statements**

The Examiner noted that The information disclosure statements filed on 04/16/04 and 07/25/06 fail to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication, or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. The Examiner remarked that the statements have been placed in the application file, but the information referred to therein has not been considered.

In reply, Applicant appreciates the Examiner's diligence in ensuring that the information disclosure statements comply with the Rules, and notes that the references associated with the noted non-compliant submissions were filed in a compliant information disclosure statement submitted on 08/17/2004, which has been signed off by the Examiner as being considered, and on 05/30/2007, which is still pending consideration.

**In the Specification**

The Examiner objected to the disclosure because of the following informalities:

The Examiner noted the use of acronyms (i.e., IEEE, RSA, USB, etc.) throughout the specification without first including a description in plain text as required.

The disclosure was objected to because it contains an embedded hyperlink and/or other form of browser-executable code. The Examiner required Applicant to delete the embedded hyperlink and/or other form of browser-executable code per MPEP 608.01.

The Examiner also noted the use of the trademark Linux® in the application, and stated that it should be capitalized wherever it appears and be accompanied by the generic

terminology. The Examiner further pointed out that although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Appropriate correction was required.

In reply, Applicant has amended the specification to first provide a description in plain text of all acronyms that are used. Applicant has in addition amended the specification to delete the embedded hyperlink and to capitalize "LINUX" and to accompany such use with generic terminology.

Accordingly, it is requested that the objections to the specification be withdrawn.

In addition, Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

**In the Claims**

**Claim Objections**

The Examiner objected to claims 7, 21, and 26 because the acronym "x86" is employed without first including a description in plain text as required.

In reply, Applicant respectfully traverses and notes that "x86" is not an acronym, but a well-known term of art that described a particular instruction set architecture that runs on x86-compatible microprocessors. However, in a good faith effort to further prosecution of this application through the Office, Applicant has amended claims 9 and 33 to recite "the instruction format for execution on an x86-compatible microprocessor" in place of "the x86 instruction format."

Consequently, it is requested that the objections to claims 7, 21, and 26 be withdrawn.

**Rejections Under 35 U.S.C. §112**

The Examiner rejected claim 10 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner noted that there is insufficient

antecedent basis to support the recited limitations "said second memory address" and "said memory." The Examiner stated that these limitations during examination will be interpreted as "a memory address" and "memory."

In reply, Applicant asserts that the Examiner's interpretation of the claim is correct in part, and that claim 10 is amended by this communication to recite "said first memory address" which has antecedent basis in claim 10 itself, and "memory" as the Examiner has correctly interpreted Accordingly, it is requested that the rejection of claim 1- be withdrawn.

The Examiner also The Examiner rejected claim 10 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner noted that there is insufficient antecedent basis to support the recited limitation "said first memory address." The Examiner stated that this limitation during examination will be interpreted as "a memory address."

In reply, Applicant has amended claim 14 by this communication to recite "a first memory address" in lieu of "a fourth memory address," which provides antecedent basis in claim 14 itself, for "said fist memory address." Accordingly, it is requested that the rejection of claim 14 be withdrawn.

**Rejections Under 35 U.S.C. §102(b)**

The Examiner rejected claims 1-6, 8-10, 12-20, and 22-25 under 35 U.S.C. 102(e) as being anticipated by Yup et al. (US2002/0191784). Applicant respectfully traverses the Examiner's rejections.

As per claim 1, the Examiner noted that Yup et al. disclose an apparatus for performing cryptographic operations, comprising:

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a provided cryptographic key be

expanded into a corresponding key schedule for employment during execution of said one of the cryptographic operations [page 3, paragraph 00281;

- keygen logic(key expansion block), operatively coupled to said cryptographic instruction, configured to direct said computing device to expand said provided cryptographic key into said corresponding key schedule [page 3, paragraph 0028]; and
- execution logic (key expansion logic), operatively coupled to said keygen logic, configured to expand said provided cryptographic key into said corresponding key schedule [page 3, paragraph 0028].

In reply, Applicant respectfully disagrees with the Examiner's characterization of Yup vis-à-vis that subject matter which is recited in claim 1. To aid in the following analysis, claim 1, as amended herein, is repeated below.

1. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a provided cryptographic key be expanded into a corresponding key schedule for employment during execution of said one of the cryptographic operations;

keygen logic, operatively coupled to said cryptographic instruction, configured to direct said microprocessor to expand said provided cryptographic key into said corresponding key schedule; and

execution logic, operatively coupled to said keygen logic, configured to expand said provided cryptographic key into said corresponding key schedule.

Applicant respectfully notes that Yup et al. do no teach a cryptographic instruction. In support of this assertion, it is noted that Applicant has carefully searched Yup et al. and reports that the term "cryptographic instruction" cannot be found therein. In fact, Yup et al. teach "A circuit includes a single circuit portion for implementing the Advanced

Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels. The circuit portion includes a circuit for individually generating, on the fly, the round keys used during each round of the AES block cipher algorithm. The circuit portion also includes shared logic circuits that implement the transformations used to encrypt and decrypt data blocks according to the AES block cipher. The single circuit portion encrypts or decrypts data blocks from each of the plurality of system channels in turn, in round-robin fashion. The circuit portion also includes a circuit for determining S-box values for the AES block cipher algorithm. The circuit additionally implements an efficient method for generating round keys on the fly for the AES block cipher decryption process. (Abstract)

It is not disputed that Yup et al. teach a circuit for implementing the AES block cipher algorithm in a system having a plurality of channels. But such a technique is roughly analogous to prior art stand-alone cryptographic processing units, the problems of which the present inventors have noted and for which the present invention is provided to overcome. With regard to how their invention is directed to process data blocks, Yup et al. are utterly silent other than to present a plurality of input registers 102 and associated control signals 103 that are coupled to a corresponding plurality of "system channels."

One skilled will appreciate that this type of configuration is troublesome in that to provide for encryption and/or decryption of data, a processor must also provide for communication with Yup et al.'s device via some system channel mechanism.

In contrast to Yup et al.'s stand-alone AES unit, claim 1 recites a cryptographic instruction that is received by a microprocessor as part of an instruction flow executing on said microprocessor. The claim continues to recite how the cryptographic instruction prescribes that a provided cryptographic key be expanded into a corresponding key schedule for employment during execution of said one of the cryptographic operations. Yup et al. do not teach or suggest an instruction, nor do they teach, allude to, or even hint at an instruction that provides for the foregoing limitation. The claim also recites keygen logic, operatively coupled to said cryptographic instruction, configured to direct said microprocessor to expand said provided cryptographic key into said corresponding key

schedule; and execution logic, operatively coupled to said keygen logic, configured to expand said provided cryptographic key into said corresponding key schedule. Although Yup et al. teach a key expansion block, as the Examiner suggests, it is not operatively coupled to a cryptographic instruction. This is because Yup et al. are silent regarding a cryptographic instruction as the present inventors have claimed and disclosed.

Based upon the above arguments, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

With respect to claims 2-6, 8-10, and 12-16, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6, 8-10, and 12-16.

As per claim 17, the Examiner noted that Yup et al. disclose an apparatus for performing cryptographic operations, comprising:

- a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes that a cryptographic key be expanded into a corresponding key schedule be employed when executing said one of the cryptographic operations [page 3, paragraph 0028]; and
- keygen logic (key expansion block), operatively coupled within said cryptography unit, configured to direct said device to perform said one of the cryptographic operations and to expand said cryptographic key into said corresponding key schedule [page 3, paragraph 0028].

Applicant respectfully disagrees with the Examiner's arguments provided above and directs attention to the arguments submitted in traversal of the rejection of claim 1. In summary, Yup et al.'s invention is a stand-alone unit, not part of a microprocessor. As such, it does not execute an instruction flow. And furthermore, the instruction flow does not provide a cryptographic instruction that prescribes, *inter alia*, that a cryptographic

key be expanded into a corresponding key schedule be employed when executing said one of the cryptographic operations.

In view of the above arguments, it is respectfully requested that the rejection of claim 17 be withdrawn.

With respect to claims 18-20 these claims depend from claim 17 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 18-20.

As per claim 22, the Examiner noted that Yup et al. disclose a method for performing cryptographic operations in a device, the method comprising:

- receiving a cryptographic instruction that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations and expanding the cryptographic key into the corresponding key schedule [page 3, paragraph 0028];

Applicant respectfully disagrees with the points asserted above and directs the Examiner's attention to the arguments submitted in traversal of the rejections of claims 1 and 17. Claim 2 recites, among other elements and limitations, within a microprocessor, receiving a cryptographic instruction that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations. As noted earlier, Yup et al. does not teach a microprocessor, nor it is taught that the microprocessor receives a cryptographic instruction that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations. This is because Yup et al. teaches a stand-alone AES unit that is fed data from system channels, and does not teach or suggest that such a unit is part of a microprocessor that receives a cryptographic instruction as part of an instruction flow executing on the microprocessor.

Accordingly, it is respectfully requested that the rejection of claim 22 be withdrawn.

With respect to claims 23-25, these claims depend from claim 22 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 23-25.

**Rejections Under 35 U.S.C. §103(a)**

The Examiner rejected claims 7, 11, 21, and 26 under 35 U.S.C. 103(a) as being unpatentable over Yup et al.. Applicant respectfully traverses the Examiner's rejections and notes that claims 97, 11, 21, and 26 depend from claims 1, 17, and 22, as appropriate, and recited limitations above and beyond those elements which have been argued above as being allowable over the prior art of record. Consequently, Applicant respectfully requests that the Examiner withdraw the rejections of claims 7, 11, 21, and 26.

## CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-26 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
**HUFFMAN PATENT GROUP, LLC**

/Richard K. Huffman/

By: _____

**RICHARD K. HUFFMAN, P.E.**
Registration No. 41,082
Tel: (719) 575-9998

08/24/2007

Date: _____